Information and Communication Technology Security and Safe Use Policy

1. Introduction

Purpose

The purpose of this Policy is to protect Dundee City Council's information and communication technology assets (IT Assets) from all threats, whether internal or external, deliberate or accidental and to meet all regulatory and legislative requirements, specifically in relation to:

- Data Protection
- Computer Misuse
- Copyright, Designs & Patents
- Telecommunications
- Obscene Publications
- Discrimination
- Intellectual Property Rights

IT Assets includes but is not limited to Council systems and equipment used to communicate both within and outside Dundee City Council eg telephones, electronic mail, voicemail, computers, internet access, the software and wiring to access those forms of communication, fax and photocopy machines.

The Council recognises that the effective, efficient and appropriate use of its IT Assets will support and improve service delivery. It therefore has a responsibility both to protect these assets' security and integrity and to ensure their safe and proper use. This policy is intended to achieve these aims. Failure to follow its terms will reduce the effectiveness of the Council's IT assets and may lead to their damage.

The policy applies to all authorised users of Dundee City Council's Corporate Network or the Corporate Internet feed supplied by Dundee City Council or any other IT assets. All users, whether employees or external third parties, must comply with its terms. Failure to do so by an employee will render them liable to disciplinary action up to and including dismissal. Failure to do so by an authorised external user is likely to result in the withdrawal of their access rights and may result in action against them or their employer to redress any loss suffered by the Council.

Users of the Education (Curriculum) Network are governed by a separate policy.

Monitoring

The Council reserves the right to monitor (eg content and level of use), record and access and/or disclose any messages or data transmitted through its systems at any time and from any location, eg

- to investigate or detect the unauthorised use of Council systems (eg breaches of this policy);
- to prevent or detect crime;
- to ensure the effective operation of the systems (eg monitoring for viruses);
- to establish the existence of facts relevant to Council business (eg communications relevant to a contractual relationship that has been entered into by use of its systems);
- to ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the Council's business; and to ensure the confidentiality, integrity and availability of Council data.

Suspected breaches of the policy will be investigated by the user's line management, with the advice and assistance of the IT Security function where necessary.

NB Security Incident Management

The aim of this policy is to enable and encourage behaviour which avoids security incidents.

However, such incidents will inevitably occur. Where they do, it is essential that they are addressed immediately and managed effectively. Section 13 of this document sets out what to do in the event of such an incident. All users must familiarise themselves with this guidance and follow it where an incident occurs.

2. Access Control

Access to systems will only be granted where it is essential for individuals to discharge their responsibilities.

All access will be authorised by the asset owner.

Special controls will apply to the use of privileged access facilities.

Access will be granted, maintained and monitored in a manner that avoids any conflict of interest between those granting the access and those with responsibility for systems maintenance.

All access rights will be reviewed at a frequency consistent with the business risks.

Managers are responsible for ensuring that their team's access rights are consistent with each individual member's duties and responsibilities.

Group passwords must not be used.

Passwords must be selected in accordance with the Password Policy.

All passwords must remain confidential to the employee.

Wherever possible, transaction accountability must be maintained.

Users must not leave computer equipment unattended that is logged on with their credentials without "locking" the computer.

Remote employees will be authenticated prior to being granted access.

Repeated unsuccessful log on attempts will lead to denial of service and subsequent investigation.

Logs of critical system activity will be maintained for subsequent independent review.

3. External Access

The Council holds an enormous amount of data relating to all aspects of local authority business. As much of this data is confidential and in some cases is highly sensitive, the Council has a duty to prevent unauthorised access to its information systems. Computer viruses and the ever-present threat from hackers mean that the IT Service must take all reasonable steps to minimise the risks associated with unauthorised access.

The Corporate IT network was originally designed primarily to meet the needs of employees working on Council premises. There is, however, an increasing demand for Council IT facilities to be available externally - to employees working at home, to external organisations and to non-employees.

Typical external access scenarios include:

- Partnerships with external organisations, eg NHS, subcontractors and funded bodies;
- Remote IT support from third party suppliers;
- Council staff working from non-Council premises;

- Non-Council staff accessing networked systems from DCC premises.

External access to Council systems raises a number of challenges at both a technical and procedural level which must be addressed if the Council's information systems are to be protected against unauthorised access. A systematic approach to assessing the risks associated with external systems access is therefore required.

Where it is believed that there is a business need for an employee to externally connect to the council, a formal request must be made to IT using a BID (Business and IT Development) Request which you can access on the IT helpdesk pages of the intranet.
https://onedundee.dundeecity.gov.uk/it/helpdesk

An application for access by an external organisation or a non-employee must be made through the Head of the Service with whom they are working.

Connection will only be made through a secure two factor VPN using 2 factor authentication to the Corporate Citrix Infrastructure.

Dial-up modems will not be used as method of connection within Council premises as this represents a potential security breach.

In certain situations users will be granted access to their desktops but this is controlled on a strict business need case by case basis.

4. Mobile Devices

When using mobile computing or communications facilities, eg notebooks, tablets, laptops, and mobile phones, special care should be taken to ensure that these devices are not compromised.

For all mobile devices:

- Don't leave your device unattended in a public area;
- Always carry it as hand luggage;
- Don't leave it visible in a vehicle;
- Don't leave it in your vehicle overnight, including in the boot;
- Be aware of the dangers of individuals viewing device screens whilst you work in a public place (shoulder surfing);
- Connect to the network as often as possible to update virus definitions (see Antivirus below);
- All mobile phones and tablets must be password protected with at least a four digit pin code.

Personal Use

Mobile devices may be used for personal texts or calls to UK landlines or mobile phones. They must not be used for any non-work-related purpose that is likely to incur 'out of plan charges' including calls and text messages to premium numbers, uploading and/or data streaming, or any form of chargeable multimedia including gaming. Staff will be liable for any 'out of plan charges' incurred for personal reasons.

5. Theft or Loss

In the event of theft, loss or any compromise of the equipment, suspected or actual:

- Identify the extent of the loss (ie which pieces of equipment are missing?).
- Notify the IT Help Desk so that any remote access capability for the equipment can be disabled.
- Notify the Police in the event of an item being stolen if you are unable to notify the IT Help Desk.

NB IT reserves the right to perform a "system wipe" on any mobile device suspected of being compromised. This will result in the permanent loss of **all data stored** on the device.

6. Passwords

Users must not share their passwords with anyone within or outside the Council. This includes IT Staff. Passwords should not be written down in plain text or stored in any manner that may compromise their confidentiality.

Specifically, passwords must not be:

- Written on or near computer equipment.
- Written in a desk diary or similar place.

Users must change passwords when they have any reason to suspect that the password may have been compromised.

Temporary passwords must be changed immediately after use.

It is good practice to use of a passphrase rather than a complex password as it is easier to remember and more difficult to break. It is therefore recommended that a passphrase containing at least three words is used.

7. Anti-Virus

All computer systems used for council business have anti-virus software installed prior to use. Automatic updates occur to ensure this software is at the appropriate level.

Laptops and tablets must be connected to the council network at least monthly to ensure these devices have the appropriate level of anti-virus software.

Unauthorised data must not be downloaded or installed on council computer systems.

Authorised data must only be downloaded from sites where there is reasonable confidence that the data will be free from viruses.

Non-Council media must be scanned for viruses prior to use.

If Council media, disks, memory sticks etc. are used on non-council equipment then these must be scanned for viruses prior to further use.

If virus infection is suspected then this must be reported to the IT Service help desk.

No copying to or from the system must then take place until any virus is cleared.

8. Storage

The IT Service has implemented a Storage Area Network as the Council's storage platform. To ensure the efficient and effective use of this facility:

- Use the Council's electronic records and document management system (CeRDMS).

- Store shared information in "team or "public" areas.

- If you are leaving the Council's employment:

  - transfer any information stored in your "home" area to an appropriate area
  - clear your email and transfer information which should be retained to an appropriate area

- If you are the manager of an employee leaving the Council ensure the above happens.

- Only store shortcuts on the desktop. Documents etc stored on the desktop will lead to delays logging in and out.

- Do not store any non-business information, data, music, images or software on any of the Council's computing facilities.

9. Backups

It is your responsibility to ensure that your files are being backed up. You should be aware that files saved solely on a PC are not backed up and could easily be lost. All files should be saved to CeRDMS, team or network shares. Files saved only to your desktop will not be backed up.

Trust the backups; do not store numerous copies of the same information.

Information and advice on backup and recovery procedures is available from the IT Service.

10. Copyright and Licence Conditions

The software used on Council computer systems is copyrighted and is used under licence agreements.

You must not:

- take copies of any software unless you are authorised to do so;

- attempt to modify software;

- load any unlicensed/unauthorised software onto Council computer systems. This includes but is not restricted to: music, video and images.

If you are in any doubt about the licence arrangements for software, clarify the position with your manager or the IT Service.

11. Internet and Email Acceptable Use

All documents and/or files are owned by the Council and not by individuals.

Email should only be used to transmit confidential or other sensitive information where both the sender and recipient are users of a secure network such as gcsx. Speak to your manager if you think you should have this facility.

Use of the Internet and e-mail is primarily for business purposes but limited personal use is allowed consistent with local management requirements. Personal use must not be carried out within working hours.

Employees **must not** register their Council email address for personal business. If this has been done previously then employees must remove their Council address.

You must not use computing facilities for the creation, display, production, or propagation of material which might be reasonably regarded as:

- offensive;
- indecent;
- of a menacing nature;
- intended to misinform and thereby cause annoyance, inconvenience, or needless anxiety in another.

The Council regards all forms of harassment as unacceptable and will deal with any complaints in accordance with its formal procedures.

The content of Internet sites browsed or downloaded must not contain anything that could be construed as offensive, discriminatory, indecent, commercially or personally defamatory.

Sent emails must not contain anything that could be construed as aggressive, racist, sexist, unsubstantiated opinion, commercially or personally defamatory or otherwise potentially offensive. Incoming external emails will be filtered through the Council's email filter to reduce the number of SPAM emails and emails that have content that could be construed as aggressive, racist, sexist, unsubstantiated opinion, commercially or personally defamatory or otherwise potentially offensive.

Caution should be taken when opening mail - especially any marked as "Possible Spam". SPAM messages should be deleted.

Incoming emails that contain anything that could be construed as aggressive, racist, sexist, unsubstantiated opinion, commercially or personally defamatory or otherwise potentially offensive should be deleted.

Employees should never open an email or click on an attachment or web link unless they are 100% sure that the sender is genuine. The email should be deleted. **If they click on the attachment or web link or are unsure about whether they have done so, then they should follow the IT Security Incident Management Procedure described at Section 13 of this policy immediately**.

All employees must maintain virus awareness.

All employees must ensure compliance with all relevant legislation.

All Internet and e-mail traffic, including attachments, and usage of the facilities may be monitored and reviewed and appropriate action taken to address breaches of this policy.

All managers are responsible for implementing the policy within their areas of responsibility.

(A guide on good practice when using email is attached as an appendix).

12. USB Memory Devices

The council discourages the use of USB memory sticks. Employees should avoid their use wherever possible.

Their small physical size, speed and ever-increasing storage capacity makes USB memory devices a convenient device to use for transferring information from one place to another. However, these very features introduce new security risks and amplify risks that already existed with floppy disks. The primary risks associated with USB memory sticks are:

- Virus Transmissions - Data sharing opens up an avenue for viruses to propagate;
- Corruption of data - Corruption can occur if the drive is not un-mounted cleanly;

- Loss of media - The device is physically small and can easily be misplaced;
- Loss of confidentiality – Data on the lost physical media can be obtained by others.

To mitigate these risks, these devices should be used sparingly and where they are used, the following must be adhered to:

USB memory devices should generally be used only to transfer non-sensitive, non-confidential information.

If sensitive, confidential information has to be transferred by this medium assistance must be sought from IT.

These devices should only be used for occasional transfer of information. If regular transfer of information is required then a request must be sent to the IT Service.

Once the transfer is complete then the information must be removed from the device.

If the device is used on non-council equipment then it must be virus checked on return to the council even if all information has been removed.

If a device is misplaced/lost then this must be reported immediately to the IT Services' Help Desk on Ext 8000, stating what information is on the device.

13. IT Security Incident Management

Overview

Potential and actual security incidents are increasing year on year. These events could have both compliance and legal consequences. This procedure has been developed to ensure that a managed and consistent framework is in place to both capture and learn from such incidents.

Types of Security Incidents

An **actual** security incident or event is defined as a breach, threat, weakness or malfunction that may have an impact upon the security of Dundee City Council information related assets. Incidents include but are not limited to:

- Unauthorised access of Council IT equipment
- Unauthorised modification of Council IT equipment
- Theft of Council IT equipment
- Introduction of malicious software on to the Council network
- Wilful damage to a Council IT equipment
- Breaches of Council Information Security Policy
- Events which have an impact on Council continuity eg denial of service attacks

Reporting a Security Incident

It is the responsibility of **all employees** to report security incidents.

Any employee identifying **a potential** security incident or weakness must promptly report it to their line manager and they or their line manager must report to the IT Help Desk. The IT Section Leader (Security) will deal with the potential incident in strict confidence.

All security incidents must be promptly reported to the IT Help Desk.

IT Help Desk
Phone: 01382 438000

https://onedundee.dundeecity.gov.uk/it/helpdesk

Appendix

Good Practice when Using Email

Communication by email is an integral part of effective service delivery. Used appropriately email is a valuable tool. Used badly, it is likely to hamper effective communications and therefore service delivery. The following is intended to help you use email well.

- Do not use email where a phone call or a face-to-face meeting is required.
- Remember that email is not generally a suitable means to send confidential or sensitive information.
- Remember that advice given in an e-mail is likely to have the same legal standing as any other written advice.
- You should not auto forward e-mails intended for the Council to an e-mail account with another Internet Service Provider.
- Check your in-box regularly but not obsessively. How you deal with received mail depends on your responsibilities and priorities but do read it, decide what you should do with it and act.
- Your service may have standards for response times. Know them and meet them.
- Where you cannot respond fully to a query within a reasonable time, let the enquirer know though a short response and tell them when you are likely to do so.
- Remember the limitations of email when composing a business message. The recipient won't see your facial expression nor hear the tone of your voice. It is not a good medium for trying to be subtle so be clear in what you say and how you say it.
- Always use a relevant subject header
- Read your message before you send it.
- Be aware of the size of the messages you send. Large messages can be very disruptive to the mail service and attaching large files can make your message so large that it consumes excessive resources, or cannot be delivered at all. As a rule of thumb, do not send messages larger than about 5Mb without first checking that the recipient can receive it and /or consulting IT about an alternative means of sending the information
- If you think a message might be capable of being misunderstood it probably will be…. so rephrase it.
- Don't use large font sizes. It can extend relatively short messages over a number of screens, making them difficult to read. Use 10 or 11 point fonts.
- DON'T EVER, EVER, WRITE IN ALL CAPITALS. It's like shouting and it looks terrible.
- Create a signature file, which will add your name, job title and contact details to the end of every e-mail you send. Keep it as short as possible - 3 or 4 lines is usually enough - and don't include irrelevant information.
- When replying to mail do not automatically include the whole of the previous message (and the message before that); include only the relevant parts. However, be careful not to change the wording of the original message.
- Verify that you are mailing to the right address. It is difficult and dangerous to guess email addresses.

Housekeeping and Records Management

- The e-mail system is not designed to be used for long term filing or storage. All e-mail messages are stored centrally and the volumes involved can quickly become unmanageable if users do not carry out regular “housekeeping”. As with traditional paper records, it is each user’s responsibility to ensure that their records are kept in good order and cleaned out regularly.

- Delete messages – received and sent - that are no longer needed.

- Save messages that you need to keep in folders and review these at reasonable intervals.

- At least monthly, review your mailboxes and folders to ensure that messages that are no longer required are deleted.

- Comply with your service’s record retention policy.

- Where, exceptionally eg pending a potential legal or other claim, messages or attachments need to be retained, they should be moved from the email system for long term electronic storage. You should seek guidance from your manager on retention requirements and timescales.